

What is claimed is:

1. A method for initializing a first device distributed with an embedded radio module using
a a server, said server having an embedded radio module, said method comprising the
steps of:

4 sending an inquiry from said server to said first device using said embedded radio
5 modules;

6 returning, from said first device, a unique device identifier of said first device, to said
7 server;

8 creating, at said server, a public key, private key pair for said first device;

9 creating, at said server, a device certificate for said first device, said device certificate
10 having a unique hardware identifier associated with said first device and a public key
11 associated with said first device;

12 transmitting said private key, and said device certificate, and a public key of a Certificate
13 Authority which signed said device certificate, to said first device; and,

14 storing said private key in non-removable protected storage at said first device.

1 2. A method as claimed in claim 1 wherein said protected storage is write-only storage
2 able to perform computations involving previously-written data.

1 3. A method as claimed in claim 1 wherein a copy of said certificate is stored in an
2 enterprise database.

1 4. A method as claimed in claim 1 wherein a copy of said certificate is stored in an LDAP
2 directory.

1 5. A method for initializing a first device distributed with an embedded radio module using
2 a server, said server having an embedded radio module, said method comprising the steps
3 of:

4 sending an inquiry from said server to said first device using said embedded radio
5 modules;

6 creating, at said first device, a public key, private key pair for said first device;

7 storing, at said first device, said private key in non-removable protected storage;

8 returning, from said first device, a unique device identifier and said public key of said first
9 device, to said server;

10 creating, at said server, a device certificate for said first device, said device certificate
11 having said device identifier and said public key; and

12 transmitting said said device certificate and a public key of a Certificate Authority which
13 signed said device certificate to said first device.

1 6. A method as claimed in claim 6 wherein said protected storage is a write-only storage
2 able to perform computations involving previously-written data.

1 7. A system for initializing a first device distributed with an embedded radio module using
2 a a server, said server having an embedded radio module, said system comprising:

3 a communications mechanism for sending an inquiry from said server to said first device
4 using said embedded radio modules, and returning, from said first device, a unique device
5 identifier of said first device, to said server;

6 a processor at said server for creating a public key, private key pair for said first device;

7 a device certificate, created at said server, for said first device, said device certificate
8 having a unique hardware identifier associated with said first device and a public key
9 associated with said first device;

10 wherein said communications mechanism transmits said private key, and said device
11 certificate, and a public key of a Certificate Authority which signed said device certificate,
12 to said first device; and, said processor stores said private key in non-removable protected
13 storage at said first device.

14 8. A system as claimed in claim 7 wherein said protected storage is write-only storage
15 able to perform computations involving previously-written data.

16 9. A system as claimed in claim 7 wherein a copy of said certificate is stored in an
17 enterprise database.

18 10. A system as claimed in claim 7 wherein a copy of said certificate is stored in an
19 LDAP directory.

20 11. An initialization system, said system comprising:

21 a first device, said first device having an embedded radio module;

22 a server, said server having an embedded radio module;

4 a communications mechanism, said communications mechanism sending an inquiry from
5 said server to said first device using said embedded radio modules;

6 wherein said first device creates a public key, private key pair for said first device, stores
7 said private key in non-removable protected storage, and returns a unique device identifier
8 and said public key of said first device, to said server;

9 said server creates a device certificate for said first device, said device certificate having
10 said device identifier and said public key; and transmits said device certificate and
11 a public key of a Certificate Authority which signed said device certificate to said first
12 device.

12. A system as claimed in claim 11 wherein said protected storage is a write-only
storage able to perform computations involving previously-written data.

13. A program for initializing a first device distributed with an embedded radio module
using a server, said server having an embedded radio module, said method comprising:

computer program code means of sending an inquiry from said server to said first device
using said embedded radio modules;

5 computer program code means of returning, from said first device, a unique device
6 identifier of said first device, to said server;

7 computer program code means of creating, at said server, a public key, private key pair for
8 said first device;

9 computer program code means of creating, at said server, a device certificate for said first
10 device, said device certificate having a unique hardware identifier associated with said first
11 device and a public key associated with said first device;

12 computer program code means of transmitting said private key, and said device certificate,
13 and a public key of a Certificate Authority which signed said device certificate, to said first
14 device; and,

15 computer program code means of storing said private key in non-removable protected
16 storage at said first device.

1 14. A program as claimed in claim 13 wherein said protected storage is write-only
2 storage able to perform computations involving previously-written data.

3 15. A program as claimed in claim 13 wherein a copy of said certificate is stored in an
4 enterprise database.

5 16. A program as claimed in claim 13 wherein a copy of said certificate is stored in an
6 LDAP directory.

7 17. A program for initializing a first device distributed with an embedded radio module
8 using a server, said server having an embedded radio module, said method comprising:

9 computer program code means of sending an inquiry from said server to said first device
10 using said embedded radio modules;

11 computer program code means of creating, at said first device, a public key, private key
12 pair for said first device;

7 computer program code means of storing, at said first device, said private key in non-
8 removable protected storage;

9 computer program code means of returning, from said first device, a unique device
10 identifier and said public key of said first device, to said server;

11 computer program code means of creating, at said server, a device certificate for said first
12 device, said device certificate having said device identifier and said public key; and

13 transmitting said said device certificate and a public key of a Certificate Authority which
14 signed said device certificate to said first device.

18. A program as claimed in claim 17 wherein said protected storage is a write-only
storage able to perform computations involving previously-written data.

00316804-052199
661250-4089760

Add A3